Executive Summary

Financial fraud is nothing new; enterprising attackers have been coming up with schemes like the “Yazoo Land Fraud” for at least the past hundreds of years. Check-kiting and socially engineered wire transfers are decades old attacks that have been frustrating banking customers and fraud examiners for years.

Online and electronic banking services have brought significant efficiencies to customers and financial institutions, but they’ve also introduced new exploit channels to the fraud pipeline.

While increasing phishing and malware attacks grab the headlines, financial fraudsters are also using hybrid attacks across multiple channels to obfuscate their trail and maximize their take. Silently performing reconnaissance work in an online account is often a first-step to executing a more lucrative offline scam. In this Note, we’ll take a brief look at how seemingly innocuous access to online account could be contributing to the rise in offline fraud and provide a look at how stopping unauthorized online access could lead to a reduction in fraud across multiple channels.
Fighting Fraud

Consider the well documented increase in phishing, keystroke logging, and password theft attacks. Tracking organization The Anti-Phishing Working Group (APWG) has identified significant increases in websites hosting malicious keystroke loggers, the most recent numbers showing a rise “by over 1,100, reaching 3,362, the second highest number recorded in the preceding 12 months.” In March 2008 ScanSafe released their Global Threat Report, reporting “password-stealing Trojans and backdoors” as the most common “final stage infectors” by a significant margin over other types of malware. Account login credentials can lead an attacker to personally identifiable information (PII) such as birthdate, mother’s maiden name, and even social security numbers that can be used later as the foundation for a full-blown identity theft attack.

As fraudsters increased their exploits, the financial services community fought back. Most institutions invested additional fraud prevention dollars, implementing stronger authentication and transaction monitoring while strengthening approval processes. Regulatory agencies and other groups provided assistance and direction such as the FFIEC Authentication Guidance, Section 114 of FACTA (also known as the “Red Flag” provision) and the Payment Card Industry Data Security Standard.

Yet, despite this vigilance, financial fraud artists continue to find new ways to steal assets from customers and institutions. To understand how to prevent the increase, it’s helpful to deconstruct methods the attackers are using. Specifically, online account reconnaissance. While a number of banks monitor post-login transactions for fraud, online attackers have wised up to the fact that performing the entire exploit online is not always the most effective way to avoid detection or execute large-scale fraud.

A far more effective method is to split up the attack cycle into a number of discrete and seemingly unconnected exploits that together form a dangerously effective whole. This approach makes tracking the cycle difficult because large portions of the attack go under the radar until after losses occur. An example of this is the Coreflood Trojan which was behind the attack that resulted in a 90,000USD unauthorized transfer from a Bank of America customer’s account. 20,000USD of the funds were withdrawn before the authorities stepped in and the account was frozen. Although Coreflood has been around for several years, it was only recently studied closely. Researchers found that the Trojan had successfully stolen account information, web page content and even PKI certificates and browser cookies. The server used in the attacks was sophisticated enough to automatically verify stolen credentials and used proxies that made logins appear to originate from the same geographic locations as the target victim account holders.
One might expect a parallel increase in online specific fraud stemming from the loss of credentials. But that’s not the case. While offline fraud is increasing (including illegal wire transfers and ACH scams) online fraud appears to be under-reported and mischaracterized. In the UK APACS reported a 33% decrease in online fraud last year.

How can this be? Online banking is increasing, (53% of U.S. households bank online today, with 67% predicted by 2012), credential theft is increasing, yet there’s a decline in online banking fraud? The answer to this apparent dichotomy may lie in the fact that the attackers are using the online information as the launch pad for the offline attacks and identity theft. To understand how, let’s take a look inside a real-life example.

Anatomy of an Attack

In this case, a real-life financial institution (FI) with over 40,000 online banking members suffered a loss. The FI had some monitoring and strong authentication services in place to keep customer accounts safe but these measures were not sufficient to prevent the fraud.

An attacker faxed a request with a valid signature to the transfer desk and fraudulently, but successfully, executed a wire transfer of funds from one of the FIs customer accounts. Viewing this exploit from the end of the cycle (Figure 1) it appears to be wire transfer fraud conducted using offline channels.

Yet as the company investigated the incident more closely, the online channel emerged as the critical entry and intelligence point for attack. Examining prior account activity investigators saw that a significant amount of funds had been transferred to the customer’s savings account from the same customer’s home equity line (HELOC). Online transfers of this sort are common and not fraudulent if executed by the authorized owner of the account. Around the time of the transfer the account activity also indicated some routine check viewings but no activity out of the normal behavior of a valid customer.
So what happened? Going back in the event chain, the attacker’s methods were revealed. Using account audit trails, the FI was able to pinpoint the suspicious logins on the account. Investigators found that during these logins checks were viewed and funds transferred from HELOC to savings. This reconnaissance activity meant that attacker now had a valid copy of the customer’s signature, obtained from the check views, and first-hand knowledge of exactly how much money was in the savings account.

Since the attacker had the correct login information (presumably stolen via a keystroke logger or other malware) the basic login process did not appear unusual. On closer examination it was determined that there were a number of anomalies associated with recent logins, such as varied, but not overly suspicious, geographic login locations and missing or mismatched cookies. Now the pieces fit together. What appeared to be an offline wire transfer fraud was in fact a multi-channel attack that started with a login using stolen credentials. (Figure 2) If the anomalous online account activity had been analyzed in real-time, the attack could have been prevented.

**Connecting the Dots**

The case study above is just one example of how activity in an online account can be used to perform offline fraud. Other examples are check fraud using information gleaned from check views and online changes to customer information such as mailing address or phone number that are exploited later as part of an identity theft scheme or phone fraud.
These multi-channel attacks are particularly hard to track because many institutions have not yet been able to completely synchronize all aspects of the account activity audit trail. Often different portions of the trail are managed by different organizations sometimes functioning over a distributed geographic area. While a “red flag” may trigger communications between the groups, seemingly normal activity most likely will not.

And the longer an attacker can fly under the radar, the more information he, or she, can collect. This includes basic account information, personal information such as address and phone number, and specifics about the level of funds in the account themselves. Consider an attacker that is monitoring an account and notices that a user receives a significant bonus check. The lurking attacker is armed with the intelligence to know precisely when to execute the fraud for maximum benefit.

Fraud examiners and investigators have the difficult task of working backwards from the point of fraud to determine where the problem started. In the case above, none of the events prior to the fraud appeared suspicious, save for the one small data point that the attacker logged in from a geographically anomalous location. In many instances, fraud is misclassified as offline only because the point of origin online cannot be correctly determined. This can lead to symptom chasing such as strengthening the rules and restrictions for phone banking transfers or check approval while the source point is not properly addressed.

Revisiting the previous example, if the FI had used online account activity analytics the scenario would look different. The login could have been protected with stronger authentication, such as using a one-time token generator, but this solution is not cost-effective or user-friendly enough for many institutions with a large customer base. Even for those use-cases where strong authentication is cost-effective, thanks to insecure storage of private keys, piggy-backing Trojans and sophisticated Man-in-the-Middle attacks, it’s often not fraud prevention effective.

Traditional online transaction monitoring works when high-value trigger events such as funds transfers occur on the account. But what about account activity that is not fund transfer based, such as check viewing and changes to personal information such as phone number or address? Writing a simple monitoring rule that alerts the security and audit team every time a user views a check would result in a flood of false positives.
Another approach is to provide stronger online account activity analytics that are transparent to the user. Building on user activity models and scoring the riskiness of the session from the very beginning at login, these analytics would have flagged the session as suspicious and alerted administrators that there was potential misuse on the account. The login could have been denied or the administrators of the online banking site could have issued alerts to other entities within the institution, such as the wire transfer group, indicating that the account was being monitored closely for fraud.

When the FI did install real-time analytics, potential fraud was prevented. In one instance anomalous logins were identified and online check viewing activity was flagged as suspicious. The FI contacted their customer immediately with this information. The customer did not think that her account credentials had been stolen, but when she ran a virus-checker a Trojan was discovered on her machine. The customer cleaned her machine and the FI changed her credential information and no losses occurred on the account.

This is not to say that all layers of the complex monitoring and fraud prevention system in effect at financial institutions are not critical and necessary. Simply, if the institution has strengthened these systems, but not considered additional protections in the online channel, a key piece of the prevention puzzle is missing - one that could prevent misuse before it starts.

**Preventing Attacks**

Online account analytics can help prevent fraud by eliminating attacker reconnaissance missions and providing administrators with early warning indicators that an account is under surveillance. Unlike token solutions, the customer is not required to carry extra hardware or perform additional steps in order to login.

Online account analytics provide stronger protection and alerting mechanisms with no overhead to the consumer. Analytic software can determine the alert levels of the online activity using available information to generate predictive models of individual user behavior against which subsequent logins and activity are assessed. Users can be authorized not just with IDs and passwords, which are easy to steal, but also with verification data inputs. Inputs such as time of login, type of activity, IP intelligence and passive device fingerprinting combined together can indicate whether or not a user is the valid account holder. Indeed, as the Coreflood Trojan shows, simple rules about one or two indicators are insufficient to stop today's fraudster. If the combination of this data is suspicious the login or activity could be rejected and an alert sent to the fraud watch team.
Post login – online activity can be analyzed in real-time. Not just transaction activity, but the seemingly innocuous activity that legitimate users engage in during authorized use, such as viewing account fund levels and changing mailing addresses. Activity analytics could dynamically learn to accommodate varied use patterns and risk appetite thresholds. For example, a customer that always logs in from the same machine using the same browser may switch browsers or begin accessing the account from a new device such as a smart phone. Simply changing location or device isn’t necessarily an indication of fraud. But combining this information with rapid logins from multiple locations, or changes to key information such as passwords and fund transfer accounts raises the aggregate risk score for this account. When the score reaches the threshold that indicates potential fraud, an alert can be triggered to the investigation team for review. Note that it is critical to set thresholds at the right level so that investigators and security teams need only inspect the accounts that are truly suspicious.

The addition of online account fraud prevention provides financial institutions with early warning alerts that can be used to strengthen the overall system and provides administrators with a way to continuously improve and strengthen the login process. In extremely suspicious cases, highly proactive measures could be triggered such as forcing a password change or even closing the compromised account and replacing it with a new one.

Online account analytics also provide key data to fraud examiners and the other organizations at the financial institution by singling out accounts that may be under surveillance and flagging them for increased monitoring. If fraud does occur in another channel, the online account analytics can be used to historically reconstruct events and help track any misuse originating in the online account. This data can also help to create more holistic protection procedures across the organization by correlating suspicious activities across multiple channels.

**Summary**

A portion of multi-channel financial fraud can be stopped before it starts by using advance analytics to monitor and score online account activity. While strong authentication, transaction monitoring and offline controls are critical for fraud prevention, savvy attackers know they’re being watched and are becoming increasingly careful about what they do online, focusing on seemingly innocuous activities as part of a greater multi-channel attack scenario.

Using online account activity analytics provides valuable intelligence to financial institutions early in the attack lifecycle. By flagging or even suspending suspicious sessions, FIs will be better equipped to prevent both on and offline fraud.
Security Curve gives companies the market and technology insight they need to make agile business moves so they can stay ahead of the security curve. Our clients benefit from targeted intelligence, comprehensive research, and focused solutions to stay ahead of the competition in a rapidly changing market.

Diana Kelley, Partner

Diana Kelley has extensive experience delivering strategic, competitive knowledge to large corporations and security software vendors. She was Vice President and Service Director for the Security and Risk Management Strategies (SRMS) service at Burton Group, the Executive Security Advisor for CA’s eTrust Business Unit, and a Manager in KPMG’s Financial Services Consulting organization.

References